Licence professionnelle *Réseaux et Sécurité*
Projets tutorés 2011-2012

Sujets proposés à l'Université de Cergy-Pontoise

1. Déploiement d'une architecture téléphonique hybride : PC-Asterisk/PABX analogique, CISCO et Panasonic + annuaire et proxy (3 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc***,** dntt(à)u-cergy.fr

Le but de ce projet est de déployer la téléphonie sur IP et analogique sur un site puis de l'interconnecter avec un autre site

a. Site 1

- Création d'un autocommutateur analogique

Vous disposez d'un PC contenant les deux cartes suivantes Digium TDM31B TDM PCI Card (3FXS-1FXO). Sur chacune de ces cartes, vous pouvez relier sur les ports FXS, un périphérique analogique FXO (téléphone, fax, etc.) et sur les ports FXO
Le logiciel Asterisk permet de transformer un tel PC en un autocommutateur PABX. Dans cette première étape, vous créerez un autocommutateur sur ce PC.
Pour cela :

- Vous installerez et configurerez Asterisk afin de prendre en charge les ports FXS.
- Vous attribuerez à votre autocommutateur le préfixe 0123 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

- Création d'un d'un réseau téléphonique IP

Vous disposez d'un autre PC ne possédant pas de cartes dédiées à la téléphonie (pas de FXS ou FXO), simplement une carte réseau Ethernet. Il s'agit ici de réaliser un PBX entièrement basé sur IP. La téléphonie sur IP s'appuie sur le protocole SIP.

- Vous mettrez en place le réseau 192.168.42.0/24 sur lequel vous connecterez votre PBX IP ainsi que deux autres PC.
- Vous créerez des lignes SIP 2000, 2001, 2002, etc. que vous attribuerez aux téléphones IP. Vous utiliserez plusieurs types de téléphones IP : un téléphone IP filaire, un téléphone IP wifi, un softphone comme ekiga + casque et micro, un téléphone USB
- Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur IP.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.
- Mettez en place et expérimentez au maximum les services offerts par Asterisk : présentation du nom, filtrage d'appel, etc.

- Création de la passerelle analogique
  - Reliez votre PC commutateur analogique au réseau IP construit dans la section précédente.
  - Faites en sorte que les téléphones IP puissent appeler les téléphones analogiques du réseau RTC et vice-versa.

b. Site 2

- Utilisation d'un autocommutateur analogique propriétaire
  Vous disposez d'un PABX/IPBX propriétaire Panasonic permettant le déploiement d'un réseau téléphonique analogique/numérique.

- Vous attribuerez à votre autocommutateur le préfixe 0145 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques et de téléphones numériques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

- Création d'un d'un réseau téléphonique IP
  Vous créerez un PBX entièrement basé sur IP en utilisant les équipements CISCO dédiés à cet effet,

c. Interconnexion de sites

- Connexion IP à IP : Réalisez l'interconnexion entre les réseaux téléphoniques IP avec l'autre site.
- Connexion RTC à RTC : A l'aide des ports FXO, réalisez l'interconnexion entre les réseaux analogiques des deux sites.

d. Fonctionnalités supplémentaires

- Utilisation de proxy et de redirecteur pour la téléphonie IP : Mettez en place un proxy et un redirecteur permettant l'enregistrement des numéros et (jabber) téléphone dans un intranet. Cette fonctionnalité est importante par rapport à l'évaluation finale du projet.
- Intégration LDAP : Vous déploierez et utiliserez un annuaire LDAP pour les services de présentation du nom, recherche numéro, etc.
- Visio-conférence: Sur votre machine Asterisk, prenez en compte le protocole H323 afin de permettre la visio-conférence. Testez.
- Modem : Un numéro de téléphone sur un des sites devra également être disponible afin de pouvoir être appelé en utilisant le réseau RTC et permettre une connectivité IP par ce biais.
- Fax : Un numéro de fax devra être offert et utilisable.

Travail demandé
Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme téléphonique qui devra être fonctionnelle, maintenable et redéployable. Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les pré-requis et les concepts notamment de téléphonie ainsi que les difficultés rencontrées, les remarques et les limitations. Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

2. IPv6 : déploiement et réseaux mobiles (3 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc***,** dntt(à)u-cergy.fr

Le but de ce projet est d'une part de déployer des réseaux IPv6 sur deux sites puis de les interconnecter, d'autre part de mettre en place la mobilité IPv6.
Référence : http ://livre.g6.asso.fr

a. Déploiement

Vous déploierez deux sites IPv6 reliés par un routeur ne supportant qu'IPv4 (et donc pas IPv6).

- Site 1

Vous utiliserez pour le site 1, le préfixe *2001:660:300f:1::/64* . Vous activerez l'autoconfiguration sans état des machines sur le site 1 en utilisant le préfixe global (par message d'annonce des routeurs).

- Site 2

Pour le site 2, le préfixe *2002:2221:4e:1::/64* . Vous mettrez en place sur le site 2 un serveur DHCPv6 pour une configuration avec état.

- Interconnexion de sites IPv6

On suppose que toutes vos machines ainsi que vos routeurs supportent les protocoles IPv4 et IPv6.

En revanche, le routeur du FAI (le routeur intersite) n'accepte que le protocole IPv4.
Il s'agit d'établir un tunnel entre les deux sites afin de leur permettre d'utiliser IPv6 entre eux.

- Services

Bien que les protocoles de transport TCP et UDP fournissent aux applications une interface indépendante du protocole IP sous-jacent (v4 ou v6), certains efforts de compatibilité ont dû être réalisées sur les applications (essentiellement au niveau des structures de programmation manipulant les adresses IP elles-mêmes).
Les grands logiciels correctement programmés (serveur HTTP Apache, serveur de courrier Postfix, navigateur Firefox, lecteur de mail Thunderbird, etc) sont tous compatibles IPv6 (ce qui n'est malheureusement pas le cas de beaucoup de logiciels alors que l'effort à faire pour être compatible est très minime).
Voici les services que vous devrez obligatoirement déployer en IPv6 :

- serveur DNS pour les zones IPv6
- Protocole HTTP avec le logiciel Apache
- Protocole SMTP avec le logiciel Postfix
- Protocole POP/IMAP

b. Mobilité

Il s'agit de permettre à un terminal mobile (un ordinateur portable) en IPv6 de changer de réseaux rapidement sans pour autant perdre sa connectivité et son accessibilité.
Vous utiliserez pour cela des bornes sans-fil et mettrez en oeuvre la pile LIVSIX (ou autre) pour parvenir à vos fins.

Travail demandé

Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme IPv6 qui devra être fonctionnelle, maintenable et redéployable. La partie mobilité IPv6 est particulièrement importante et devra être soigneusement étudiée.
Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les prérequis et les concepts notamment de téléphonie ainsi que les difficultés rencontrées, les remarques et les limitations.
Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

3. Plate-forme de travail collaboratif : eSupPortal, LDAP, Serveur CAS (3 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc,* dntt(à)u-cergy.fr

Le but de ce projet est de réaliser la mise en place d'un ENT (environnement numérique de travail).

Dans le cadre du déploiement d'un espace numérique de travail (ENT), il s'agit de pouvoir permettre aux utilisateurs répertoriés dans un annuaire LDAP, un accès à différents services.

L'utilisateur doit pouvoir être identifié qu'une seule fois (SSO - Single Sign On) auprès d'un serveur CAS (Central Authentfication Service) lors de son premier accès à un des services. Par la suite, une fois l'utilisateur identifié et authentifié, celui-ci aura accès -sans authentification supplémentaire- à l'ensemble de son espace numérique de travail.

Celui-ci doit obligatoirement comporter les services suivants :

- configuration du profil utilisateur
- accès à sa boite aux lettres
- un espace de stockage pour gérer ses documents
- un calendrier
- une gestion de ses pages web
- didacticiel (moodle)

Une interaction avec les autres utilisateurs doit également être possible :

- partage de fichiers
- chat et messagerie
- forum

Vous pourrez à cette fin, utiliser les solutions libres OpenPortail/eSupPortail avec ses nombreux portlets.

Son objectif premier est de fournir un espace numérique de travail modulaire, avec un accès unique et ergonomique à différents services et diverses sources d'informations et ressources numériques.

Travail demandé
Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme ENT qui devra être fonctionnelle, maintenable et redéployable.

Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les prérequis et les concepts notamment d'authentification SSO ainsi que les difficultés rencontrées, les remarques et les limitations.

Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

4. Déploiement d'un nuage (cloud) avec OpenNebula (3 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc,* dntt(à)u-cergy.fr

Le but de ce projet est de déployer un nuage (cloud).
Référence : http ://opennebula.org

Le concept d'informatique en nuage (cloud computing) constitue en la déportation sur des serveurs distants des traitements informatiques traditionnellement localisés sur les postes des utilisateurs.

Les entreprises disposant de moyens suffisants peuvent monter leur propre nuage afin d'offrir une architecture évolutive à leurs employés et leurs clients. Ce nuage peut alors être public (accessible à l'extérieur de l'entreprise) ou privé (restreint aux limites de l'entreprise).

Le stockage de fichiers est probablement l'un des services les plus connus déporté dans le nuage. Les services de stockage disposent de fermes de serveurs à plusieurs endroits dans le monde et enregistrent vos fichiers à plusieurs endroits, de manière à ce que vous y ayez accès de n'importe quel ordinateur, n'importe où sur la planète. Tout ce dont vous avez besoin, c'est d'un logiciel pour accéder à votre espace de stockage ou d'un navigateur Web.

OpenNebula.org est un projet open-source visant à renforcer l'industrie outil standard ouvert informatique source nuage de gérer la complexité et l'hétérogénéité des données distribuées infrastructures du centre.
OpenNebula est composé des éléments principaux suivants :

- Le dépôt d'images (Image Repository) permet de mettre en place et partager des images, qui peuvent être des systèmes d'exploitation ou de données, pour être utilisé facilement dans les machines virtuelles.
- Le dépôt de modèle (Template Repository) permet d'enregistrer les définitions de machine virtuelle dans le système, afin d'être instancié plus tard, comme des instances de machines virtuelles.
- La mise en réseau virtuelle (Virtual Networking) est prévue pour interconnecter des machines virtuelles. Ces réseaux peuvent être définis comme des réseaux fixes ou à distance.
- Des interfaces en ligne de commande (CLI) et graphique (Sunstone GUI)

a. Fonctionnalités générales d'Open Nebula

OpenNebula 1.2 supporte les plateformes de virtualisation Xen et KVM ainsi que le service "on-demand" d'Amazon EC2. Parmi ses fonctionnalités : gestion centralisée des machines virtuelles et des ressources physique, répartition de charges, extension des capacités par ajout de serveurs physique. Les fonctionnalités principales sont :

- *Interfaces et API* : OpenNebula fournit de nombreuses interfaces différentes (ligne de commande et interface graphique SunStone) qui peuvent être utilisés pour interagir avec les fonctionnalités offertes pour gérer les ressources physiques et virtuelles.
- *Utilisateurs et groupes* : OpenNebula en charge les comptes d'utilisateurs et groupes, ainsi que l'authentification et les mécanismes d'autorisation différents. Cette fonctionnalité peut être utilisée pour créer des compartiments isolés au sein du même nuage, la mise en oeuvre multi-location. En outre, un mécanisme d'accès puissante liste de contrôle est en place pour permettre la gestion des rôles différents,

permettant une autorisation à grain fin l'octroi.

- *Réseaux* : Un sous-système réseau facilement adaptable et personnalisable est présent dans OpenNebula afin de mieux intégrer les exigences spécifiques du réseau de centres de données existants. Prise en charge de VLAN et Open vSwitch sont _également présentes.
- *Hôtes et virtualisation* : les hyperviseurs sont supportés dans le gestionnaire de virtualisation, avec la possibilité de contrôler le cycle de vie des machines virtuelles, ainsi que leur suivi. Ce contrôle s'applique également aux hôtes physiques.
- *Stockage et Images* : OpenNebula est suffisamment flexible pour supporter autant de configurations différentes de stockage d'images possibles. Le sous-système de stockage peut être configuré pour supporter les systèmes de fichiers non partagés et partagés, ainsi qu'un large éventail d'arrangements différents des serveurs d'images.

b. Déploiement

A l'aide de machines physiques sur lesquelles vous déploierez plusieurs machines virtuelles, vous créerez un nuage à l'aide d'Open Nebula. Votre plateforme devra satisfaire aux contraintes suivantes :

- Ce nuage devra supporter plusieurs systèmes d'exploitation (dont un Windows XP ou seven, un Windows Server, un linux et un FreeBSD).
- Vous créerez une base d'utilisateurs et groupes authentifiés.
- Vous supporterez des systèmes de fichiers partagés.

Pour cela, vous considérerez 2 sites virtuels d'entreprise ainsi que des utilisateurs nomades.
Chaque site virtuel doit comporter :

- son propre réseau virtuel
- différents systèmes d'exploitation
- ses utilisateurs
- ses services publics
- ses services privés
- ses bases de données
- ses systèmes de fichiers partagés.

Les accès et les droits d'accès vers les sites seront importants. L'administration du nuage devra être démontrée de façon fine. Les bases de données déployées seront particulièrement étudiées.

Travail demandé

Vous répondrez _a toutes les exigences demandées en déployant soigneusement votre plateforme OpenNebula qui devra être fonctionnelle, maintenable et redéployable. Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les prérequis et les concepts notamment de cloud computing ainsi que les difficultés rencontrées, les remarques et les limitations. Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

5. Domaine Active Directory, DMZ, routeur et FTP (2-3 élèves)

Tuteur : *Guillaume Renier,* guillaume.renier(à)u-cergy.fr

Contexte

Une entreprise dispose d'un réseau local, d'une DMZ et est connecté à l'internet par l'intermédiaire d'un routeur. Un domaine AD est présent configuré pour l'entreprise. Les contrôleurs sont accessible uniquement sur le réseau local de l'entreprise. Chaque employé de l'entreprise dispose d'un compte sur le domaine AD.

Il est possible d'ouvrir des ports de la DMZ vers le réseau local (et donc les contrôleurs de l'AD).

Présentation

L'entreprise veut installer un serveur FTP dans la DMZ qui authentifiera les utilisateurs par l'intermédiaire de l'AD. Ce serveur doit, si possible, créer dynamiquement un répertoire personnel pour chaque utilisateur. Sinon il suffit de définir un répertoire unique accessible pour tous les utilisateurs.

Objectifs

Les contrôleurs AD 2008S peuvent être configurés en lecture seule. Les ouvertures de ports entre la DMZ et

le réseau local ne se feront que vers un contrôleur 2008S en lecture seule. Le réseau local dispose donc d'au moins deux contrôleurs W2008S dont au moins 1 est en lecture seule et au moins 1 est en lecture/écriture.

Le serveur FTP doit être un logiciel libre au sens large du terme. Il doit être installé sur un serveur UNIX (linux, FreeBSD, macOS...) et utiliser une authentification par PAM.

PAM doit être configuré pour utiliser :
- Soit un module pour RADIUS qui sera configuré pour utiliser un serveur RADIUS sur le serveur 2008.
- Soit un module LDAP qui sera configuré pour se connecter sur l'AD su serveur en lecture seule.

Le serveur FTP doit pouvoir être utilisé depuis l'internet et depuis le réseau local.

Les étudiants devront configurer 4 serveurs : 1 contrôleur 2008S en lecture/écriture, 1 contrôleur 2008S en lecture seule, 1 routeur (matériel ou logiciel) et un serveur UNIX. Le tout pouvant se faire sur des systèmes virtualisés.

Extension possible
La connexion sur le serveur FTP pourra se faire en SFTP ou en FTPS.

La connexion sur les répertoires personnels sur le serveur FTP pourront être accessible en NFS, CIFS depuis le réseau local. Le but de ce projet est de réaliser la mise en place d'un ENT (environnement numérique de travail).

Sujets proposés à l'EPMI

6. Déploiement de firmware Cisco (3 élèves)
Tuteur *Alex Falzon,* a.falzon(à)epmi.fr

Objectif : Explorer les méthodes de déploiement de firmware Cisco et en mettre une en place:

Faire un tour d'horizon sur les logiciels de référence existants.

Matériel : 1 routeur Cisco, 1 Switch Cisco, une Borne WIFI CISCO 1 PC (Choix de l'os et de la distribution)

7. Sécurité d'une infrastructure réseaux (2 élèves)
Tuteur *Alex Falzon,* a.falzon(à)epmi.fr

Objectif : Mettre en place une plateforme d'authentification RADIUS

Effectuer :

- un comparatif sécuritaire des modes d'authentifications sur les équipements réseaux.
- une sécurisation de l'accès au serveur Radius.
- une réflexion sur une architecture hautement sécurisé et adapté à un parc de plusieurs milliers d'équipements réseaux.

Matériel : 1 routeur Cisco, 1 switch Cisco, 1 serveur sous linux (Choix de l'os et de la distribution)

8. Management et supervision des réseaux (3 élèves)
Tuteur *Alex Falzon,* a.falzon(à)epmi.fr

Objectif : Explorer les moyens de supervisions de réseaux via le protocole SNMP V2 largement utilisé et effectuer un comparatif avec la version plus sophistiquée SNMP V3 :

Lister des OID utiles pour le management des équipements réseaux Cisco.

Réalisation de sondes SNMP sur du matériel réseau:

- pour l'injection et la diffusion de configuration sur les routeurs Cisco.
- pour la récupération des mots de passe oubliés sur les équipements réseaux
- pour la mise en base d'informations sur les interfaces, l'adressage et les caractéristiques hard et soft des équipements réseaux.

Faire un tour d'horizon sur les logiciels de référence existants.

Matériel : 1 routeur Cisco, 1 Switch Cisco, 1 serveur sous linux (Choix de l'os et de la distribution)

9. Messagerie collaborative unifiée (3 élèves)
Tuteur *G. Vernet,* g.vernet(à)caspeo.fr

Objectif : En vous basant sur les outils issus du monde open source, vous mettrez en place une solution de messagerie collaborative

Votre outil multi plateforme devra intégrer une authentification forte.

Matériel : 1 serveur avec un OS virtualisé (Choix de l'os et de la distribution)

10. Réseau de stockage redondant (3 élèves)
Tuteur *G. Vernet*, g.vernet(à)caspeo.fr

Objectif : Mettre en place une structure de sauvegarde déporté et sécurisée.

Vous ferez un tour d'horizon des méthode de sauvegardes.

Matériel : 1 NAS DELL , un serveur linux